Web Images Video Maps News Shopping Gmail more ▾ Sign in

Google symmetric key trap door Search Advanced Search Preferences

Web Show options... Results **1** - **10** of about **18,400** for **symmetric key trap door**. (**0.39** seconds)

Virtual private networks: making the right connection - Google Books Result
by Dennis Fowler - 1999 - Computers - 222 pages
Obviously, the **trap door** one-way functions used in public **key** encryption are much more complex. In the case of RSA encryption, the public **key** is the **trap ...**
books.google.com/books?isbn=1558605754...

PSEC: Provably Secure Elliptic Curve Encryption Scheme (Submission ...
PSEC-2 is a public-**key** encryption system that uses the elliptic curve ElGamal **trapdoor** function, two random functions (hash functions) and a **symmetric**- **...**
grouper.ieee.org/groups/1363/P1363a/contributions/psec.pdf - Similar pages

Numb3rs Season 3 Episode 11: Killer Chat
Symmetric key cryptography was the only kind of cryptography publicly known **...** the existence of a type of mathematical functions called **trapdoor** functions. **...**
www.math.cornell.edu/~numb3rs/lipa/killer_chat.html - 12k - Cached - Similar pages

Notes for Lectures 12--14 1 General One-Way and **Trapdoor** Functions
Thus, one-way functions suffice for **symmetric** encryption. However, they do not suffice for public-**key** encryption: you really need the **trapdoor** to be able to **...**
www.cs.bu.edu/~reyzin/teaching/f04cs538/oldnotes/notes12-14.pdf - Similar pages

Symmetric Key Cryptography
LEDA covers the following aspects of **symmetric key** cryptography: **....** that the developers of LEDA did not put any **trap-doors** into the code which allow them **...**
www.algorithmic-solutions.info/leda_manual/**Symmetric_Key**_Cryptography.html - 18k - Cached - Similar pages

An Introduction to Cryptography - Google Books Result
by Richard A. Mollin - 2000 - Computers - 373 pages
The very heart of the Diffie-Hellman idea is the use of **trapdoor** one-way **...** secret **key** is reserved for use in association with **symmetric-key** cryptosystems. **...**
books.google.com/books?isbn=1584881275...

Explanation of the Three Types of Cryptosystems - GIAC Research in ...
Feb 6, 2007 **...** A major challenge associated with **symmetric key** cryptosystems is the **...** using the computation of large logarithms as a **trapdoor** function. **...**
www.giac.org/resources/whitepaper/cryptography/52.php - 37k - Cached - Similar pages

Electronic Notes in Theoretical Computer Science : A New Rabin ...
May 20, 2006 **...** A New Rabin-type **Trapdoor** Permutation Equivalent to Factoring **.....** Hashing, evaluations ofthe **key** derivation function and the **symmetric key ...**
linkinghub.elsevier.com/retrieve/pii/S1571066106002945 - Similar pages
by K Schmidt-Samoa - 2006 - Cited by 1 - Related articles

Public **Key** Cryptography Tutorial
These public **key**-private **key** pairs are **trap door** one way functions i.e. its very easy to **...** Other ciphers, such as those used for **symmetric key** encryption, **...**
securitytube.net/Public-**Key**-Cryptography-video.aspx - 21k - Cached - Similar pages

Web Images Video News Maps **more »**

trap door key generat* 1776 - 2004 Search Ad Sc Sc

● Search only in Engineering, Computer Science, and Mathematics.

○ Search in all subject areas.

Scholar **All articles** - Recent articles Results **1** - **10** of about **2,890** for trap door key **generat***. (**0.31**

Did you mean: trap door key ***generator****

New directions in cryptography- ▶unam.mx [PDF]
W Diffie, M Hellman - IEEE Transactions on Information Theory, 1976 - ieeexplore.ieee.org
... introduce the even more difficult problem of **trap** doors. **...** number **generator** (eg, a noisy diode) for **generat**,ing K **...** of this kind, the problem of **key** distri- bution **...**
Cited by 6254 - Related articles - Web Search - All 112 versions

A method for obtaining digital signatures and public-**key** cryptosystems- ▶mit.edu [PDF]
RL Rivest, A Shamir, L Adleman - Communications of the ACM, 1978 - portal.acm.org
... It is not based on a **trap-door** one-way permutation **... generate** the encryption and decryption keys, such that the decryption **key** is never printed out (even for its **...**
Cited by 7646 - Related articles - Web Search - Library Search - All 113 versions

How to leak a secret- ▶uwaterloo.ca [PDF]
RL Rivest, A Shamir, Y Tauman - Lecture Notes in Computer Science, 2002 - Springer
... but we have to modify it slightly in order to use **trapdoor** one way **...** 3.1 RSA **Trap-Door** Permutations Each ring member A i has an RSA public **key** P i = (n i ,e i **...**
Cited by 384 - Related articles - Web Search - BL Direct - All 9 versions

[BOOK] Foundations of Cryptography II: Basic Applications
O Goldreich - 2004 - Cambridge University Press
Cited by 205 - Related articles - Web Search - Library Search

Designated verifier proofs and their applications- ▶nctu.edu.tw [PDF]
M Jakobsson, K Sako, R Impagliazzo - Lecture Notes in Computer Science, 1996 - Springer
... We demon- strate how a **trapdoor** commitment scheme can be uscd to construct designated **...** Example **Trap-door** coiiiiiiitnient scheme 1. [4] Secret **key** of ihe **...**
Cited by 341 - Related articles - Web Search - BL Direct - All 12 versions

Key-privacy in public-**key** encryption- ▶ucsd.edu [PDF]
M Bellare, A Boldyreva, A Desai, D Pointcheval - Lecture Notes in Computer Science, 2002 - Springer
... based scheme, I might include, in addition to k, a global prime number and **generator** of a **...** (In cases where the family is not **trapdoor**, the secret **key** is sim **...**
Cited by 134 - Related articles - Web Search - BL Direct - All 15 versions

How to enhance the security of public-**key** encryption at minimum cost- ▶future.co.kr [PDF]
E Fujisaki, T Okamoto - Lecture Notes in Computer Science, 1999 - Springer
... practical public-**key** encryption scheme se- mantically secure against adaptive chosen-ciphertext attacks (IND-CCA2) is to convert from a primitive **trap-door** one **...**
Cited by 152 - Related articles - Web Search - BL Direct - All 17 versions

How to share a function securely
A De Santis, Y Desmedt, Y Frankel, M Yung - Proceedings of the twenty-sixth annual ACM symposium on ...,

Web Images Video Maps News Shopping Gmail more ▾ Sign in

Google goran selander key generation Search Advanced Search Preferences

Web Show options... Results **1** - **10** of about **515** for **goran selander key generation**. (**0.29** seconds)

(WO/2005/038818) EFFICIENT MANAGEMENT OF CRYPTOGRAPHIC **KEY** GENERATIONS
SELANDER, **Göran** [SE/SE]; (SE) (US Only). LINDHOLM, Fredrik [SE/SE]; (SE) (US Only).
... at **key** update, **key** information of an older **key generation** by the **key ...**
www.wipo.org/pctdb/en/wo.jsp?wo=2005038818 - 16k - Cached - Similar pages
by G SELANDER - 2005 - Cited by 1 - Related articles - All 6 versions

Efficient management of cryptographic **key** generations invention
Inventors: **Goran Selander**, Fredrik Lindholm, Magnus Nystrom **...** While it is easy to indicate the **key generation** being used, it may be difficult or even **...**
www.freshpatents.com/Efficient-management-of-cryptographic-**key-generations**-dt20070607ptan20070127719.php - 34k - Cached - Similar pages

ITU-T Workshop on Digital Identity for NGN
Göran Selander (Ericsson, Ambient Networks project): Application of Cryptographic **...** Identification of **key** hurdles towards harmonizing views relating to digital identity: How can we bring digital identity to next-**generation** networks? **...**
www.itu.int/ITU-T/worksem/ngn/200612/programme.html - 19k - Cached - Similar pages

ITU-T Workshop on Digital Identity for NGN
Speaker: **Göran SELANDER**, Ericsson Research. Session: 4 - Projects on Digital Identities for Next **Generation** Networks **...** Public **key** certificates are commonly used to assert an identity or an attribute of the owner of a cryptographic **...**
www.itu.int/ITU-T/worksem/ngn/200612/abstracts.html - 39k - Cached - Similar pages
More results from www.itu.int »

Efficient management of cryptographic **key** generations - Patent ...
Selander, **Goran** (Stockholm, SE) Lindholm, Fredrik (Alvsjo, SE) **...** The method of claim 2, wherein said predetermined **key generation** is a master **key ...**
www.freepatentsonline.com/y2007/0127719.html - Similar pages
by G Selander - 2007 - Cited by 1 - Related articles - All 6 versions

Secure implementation and utilization of device-specific security ...
Selander, **Goran** (Stockholm, SE) Nerbrant, Per-olof (Osterkar, SE) **....** Reference [3] mentions so-called on-board **key generation** in connection with smart **...**
www.freepatentsonline.com/y2006/0101288.html - Similar pages
by B Smeets - 2006 - All 5 versions
More results from www.freepatentsonline.com »

Attaching an IMS Subscriber to an Unknown Foreign Network
of the session **key**. Note that the attachment procedure makes it possible for the user to encrypt **... Göran Selander** for comments and suggestions. References **... Generation** Partnership Project Technical Specification,. TS 23.234 V7.5.0. **...**
ieeexplore.ieee.org/iel5/4545485/4545486/04545520.pdf - Similar pages
by S Heikkinen - 2008 - Related articles - All 3 versions

Ambient Network Attachment
A **key** aspect of the project is to establish a common control layer for various network types, **... Göran Selander ... generation** networks and within the AN project **.....** [7] **Göran** Klang,